

December 20, 2023

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

U.S. DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
LONG ISLAND OFFICE

IN THE MATTER OF THE SEARCH OF
A LIGHT GRAY GOOGLE PIXEL
PHONE CURRENTLY LOCATED AT 135
PINELAWN ROAD, MELVILLE, NY
11747.

TO BE FILED UNDER SEAL

APPLICATION FOR A
SEARCH WARRANT FOR AN
ELECTRONIC DEVICE

Case No. 23-MJ-01126 (JMW)

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Colleen Sheehan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and have been since March 2018. I am currently assigned to the Crimes Against Children and Human Trafficking Unit (the “Task Force”), of which I have been a member for approximately the past two years. As a member of the Task Force, I investigate criminal violations relating to the sexual exploitation of children, including the illegal production, distribution, transportation, receipt, and possession of child pornography, the transfer of

obscene materials to minors, and the use of electronic means to persuade, induce, entice and coerce minors to engage in sexual activity.

3. I have been involved in numerous child exploitation investigations and am familiar with the tactics used by individuals who engage in such offenses. As part of my responsibilities, I have participated in the execution of multiple search warrants relating to child exploitation offenses, including search warrants for electronic devices, and have effectively used the results of the searches in connection with the prosecution of offenders.

4. The statements in this affidavit are based on my personal knowledge, on information I have received from other law enforcement personnel, and from persons with knowledge regarding relevant facts. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a Google Pixel Phone (the “Device”) with a single front-facing camera at the top of the screen and a scratch on the lower right half of the screen. The back of the Device is light gray with a “G” logo in the middle, and there is a metal strip across the back of the Device where the Device’s rear-facing cameras are located. The Device is currently located at the FBI field office at 135 Pinelawn Road, Melville, New York 11747. Two pictures of the Device follow:



6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. The Task Force is investigating DOUGLAS ENGSTROM for the following violations of federal law: Title 18, United States Code, Sections 1470 (transfer of obscene material to minors), 2422 (coercion and enticement of minors), and 2423 (transportation of minors) (together, the “SUBJECT OFFENSES”). Based on the facts set forth below, I believe that the Device will contain and constitute evidence, fruits, and instrumentalities of the SUBJECT OFFENSES.

8. On or about December 6, 2023, a member of the Task Force (the online covert employee, or “OCE”) posed undercover as a 13-year-old girl on a free mobile messaging application that allows users to anonymously transmit and receive messages, photos, videos, and other content, both publicly or privately to a specific user (the “app” or “application”). An individual with the username “bleepbloorp” contacted the OCE on the application in response to a post in which she claimed to no longer need dental braces. The OCE represented in multiple messages with the bleepbloorp account that she was a 13-year-old girl in school. During messaging, the user of the bleepbloorp account represented to the OCE that he was named Doug, that he was 36 years old, and that he lived in Maryland.

9. The user of the bleepbloorp account repeatedly expressed interest in engaging in sexual conduct with the OCE. While the user of the bleepbloorp account first made these statements on the app, he later provided the OCE with a cell phone number and continued making similar statements to the OCE via text message. In these text messages, he expressed interest in having oral, anal, and vaginal sex with the OCE, including while she was drunk or unconscious. He also sent the OCE pictures and videos of himself masturbating and requested that she send him pictures of herself. Some of the pictures that he requested were sexually suggestive in nature, such as pictures of the OCE in her underwear.

10. Based on information associated with the cell phone number provided by the user bleepbloorp, as well as facial photographs sent by that user, law enforcement

agents determined that the user of the bleepbloorp account was the defendant DOUGLAS ENGSTROM, a 36-year-old residing in Maryland.

11. In conversations with DOUGLAS ENGSTROM, the OCE represented that she lived in Valley Stream, New York. ENGSTROM expressed interest in visiting her in Valley Stream on December 16, 2023 to engage in the sexual conduct described above. On or about December 14, 2023, ENGSTROM informed the OCE that he had booked a hotel and flight tickets for that purpose.

12. While in transit from Maryland to New York, DOUGLAS ENGSTROM asked the OCE to call him so that he could hear her voice, which I interpret as an attempt to confirm that the OCE was in fact a 13-year-old girl rather than an undercover law enforcement officer. The OCE called him at the cell phone number that he had been using to send the text messages described above, and he did not appear to realize that she was in fact an undercover officer.

13. Law enforcement officers used the information provided to the OCE by DOUGLAS ENGSTROM to determine the flight by which he would arrive at John F. Kennedy International Airport. When ENGSTROM arrived at the airport, law enforcement officers determined that his appearance matched the appearance of the individual depicted in the photographs sent by the user of the bleepbloorp account. Law enforcement agents then surveilled ENGSTROM at the airport until he departed in a taxi or ridesharing service vehicle. ENGSTROM text messaged the OCE from the vehicle and informed her that he would meet her at the Long Island Railroad train station at Valley Stream.

14. Law enforcement officers arrested ENGSTROM shortly after he arrived at the Valley Stream train station as agreed upon. ENGSTROM had the Device open in his hand and appeared to be in the process of text messaging the OCE to determine her location.

15. Based on my training and experience, child exploitation offenses are frequently committed by means of electronic devices such as computers and cell phones, and evidence of those crimes such as communications, photographs, and videos may also be found on such devices.

16. In this particular case, I believe that the Device is associated with the cell phone number that ENGSTROM used to call and text message the OCE leading up to his arrest, as well as to send obscene photos and videos of him masturbating. As ENGSTROM also used a mobile text messaging application, I believe that ENGSTROM used the Device to send messages via the mobile messaging application, and that evidence of those messages and the existence of the application on his phone will be found on the Device. The Device will also likely contain information regarding the booking of the flight and hotel ENGSTROM reserved for the purpose of engaging in sexual activity with a minor as well.

17. The Device is currently in the lawful possession of the FBI. It came into the FBI's possession incident to the December 16, 2023 arrest of ENGSTROM described above.

18. The Device is currently in storage at 135 Pinelawn Road, Melville, New York 11747. In my training and experience, I know that the Device has been stored in a

manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or

locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also

include global positioning system (“GPS”) technology for determining the location of the device.

20. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

- f. I know that when an individual uses an electronic device to communicate with minors for the purpose of engaging in illicit sexual conduct, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. I know from my training and experience that some models of mobile devices offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is often called Touch ID. I also know that certain models of mobile devices offer their users the ability to unlock the device via the use of facial recognition

(through infrared and visible light scans) in lieu of a numeric or alphanumeric passcode or password. This feature is often called Face ID.

25. If a user enables Touch ID on a given device, the user can then use any of the registered fingerprints to unlock the device. If a user enables Face ID on a given mobile device, he or she can unlock the device by raising the device to his or her face, or tapping the screen. In my training and experience, users of devices that offer Touch ID or Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents.

26. The passcodes or passwords that would unlock the Device are not known to law enforcement. Thus, it will likely be necessary to press the fingers of the user of the Device to the device's Touch ID sensor, or hold the Device in front of the user's face to activate the Face ID sensor, in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the Device via Touch ID or Face ID is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

27. I also know from my training and experience that certain mobile devices have a feature that allows a user to erase the contents of the device remotely. By logging into the Internet, the user or any other individual who possesses the user's account information can take steps to completely wipe the contents of the device, thereby destroying

evidence of criminal conduct, along with any other information on the device. The only means to prevent this action is to disable the device's ability to connect to the Internet immediately upon seizure, which requires either access to the device itself to alter the settings, or the use of specialized equipment that is not consistently available to law enforcement agents at every arrest.

28. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of ENGSTROM to the Touch ID sensor of the Device, or hold the Device in front of ENGSTROM's face (and, if necessary, hold ENGSTROM in place while holding the Device in front of his face), for the purpose of attempting to unlock the device via Touch ID or Face ID in order to search the contents as authorized by this warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

30. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Colleen Sheehan

Colleen Sheehan
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me @ 2:16pm by Facetime
on December 20, 2023:

/s/

HONORABLE JAMES A. WICKS
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK



ATTACHMENT A

The property to be searched is a Google Pixel Phone with a single front-facing camera at the top of the screen and a scratch on the lower right half of the screen, hereinafter the “Device.”

The back of the Device is off-white with a “G” logo in the middle, and there is a metal strip across the top half of the back of the Device, where the Device’s rear-facing cameras are located. The Device is currently located at the FBI field office at 135 Pinelawn Road, Melville, New York 11747. Two pictures of the Device follow:



The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 1470 (transfer of obscene material to minors), 2422 (coercion and enticement of minors), and 2423 (transportation of minors) (together, the “SUBJECT OFFENSES”) and involve DOUGLAS ENGSTROM since December 6, 2022, including:

- a. Records and information relating to sexual contact with minors;
- b. Records and information relating to the transfer of obscene materials to minors;
- c. Records and information relating to communications with minors regarding sexual conduct;
- d. Records and information relating to the mobile messaging application account with the username “bleepbloorp”;
- e. Records and information relating to the purchase of tickets for a flight to John F. Kennedy International Airport in December 2023;
- f. Records and information relating to the booking of a hotel in New York in December 2023.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of ENGSTROM onto the Touch ID sensor of the Device, or hold the Device in front of ENGSTROM’s face to activate the Face ID sensor (and, if necessary, hold ENGSTROM in place while holding the Device in front of his face), in order to gain access to the contents of the Device as authorized by this warrant.